EXHIBIT
J

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Blayn W. Beenau, *et al.*	§	Atty.Dkt.No.:	6857-23203
Serial Number:	15/187,196	§	Examiner:	Reagan, James A.
Filing Date:	June 20, 2016	§	Group/Art Unit:	3621
Title:	METHODS, APPARATUS AND COMPUTER PROGRAM PRODUCTS FOR SECURELY ACCESSING ACCOUNT DATA	§	Conf. No.	9874

****CERTIFICATE OF E-FILING TRANSMISSION****

I hereby certify that this correspondence is being transmitted via electronic filing to the United States Patent and Trademark Office on the date shown below:

On: July 26, 2017 /Paul T. Seegers/
Date Paul T. Seegers, # 66,621

RESPONSE TO OFFICE ACTION MAILED APRIL 5, 2017

This paper is submitted in response to an Office Action of April 5, 2017, to further highlight why the application is in condition for allowance.

Please amend the case as listed below.

IN THE CLAIMS:

The following is a current listing of claims and will replace all prior versions and listings of claims in the application. Please amend the claims as follows:

1-22. (Canceled)

23. (Previously Presented) A method, comprising:

generating, at a browser toolbar, a cryptographic key usable to decrypt encrypted account information of an account holder, wherein the account information is usable to conduct a transaction with the account holder;

sending, by the browser toolbar, a request for the account information to a secure database that stores the account information;

using, by the browser toolbar, the cryptographic key to decrypt encrypted data received from the secure database, wherein the encrypted data includes the account information;

securely storing, by the browser toolbar, the account information at the browser toolbar; and

providing, by the browser toolbar, the account information to a web service in response to a request.

24. (Previously Presented) The method of claim 23, wherein the generating further comprises:

generating a public key pair having a public key and a private key, wherein the private key is the cryptographic key; and

transmitting the public key to the secure database for encrypting the account information.

25. (Previously Presented) The method of claim 23, wherein the securely storing further comprises:

in response to providing the account information to the web service, deleting the stored account information from the browser toolbar.

26. (Previously Presented) The method of claim 23, wherein the cryptographic key is generated based on one or more user attributes.

27. (Previously Presented) The method of claim 23, further comprising:

prior to receiving the encrypted data, the browser toolbar providing credentials of the account holder to a server configured to verify that the account holder is permitted to access the account information.

28. (Previously Presented) The method of claim 23, wherein the providing includes the browser toolbar completing one or more fields on a web page.

29. (Previously Presented) The method of claim 23, further comprising:

prior to providing the account information to the web service, the browser toolbar presenting a plurality of transaction instruments associated with the account holder; and

the browser toolbar receiving a selection of one of the plurality of transaction instruments to be provided to the web service.

30. (Previously Presented) A non-transitory computer readable medium having program instructions stored therein that are executable by a computing device to implement a browser toolbar that performs operations comprising:

analyzing a web service to determine a request for account information associated with an account holder, wherein the account information is usable to conduct a transaction with the account holder;

producing a public key pair having a public key and a private key;

transmitting the public key to a remote database for encrypting the account information;

receiving an encrypted version of the account information from the remote database;

decrypting the encrypted version of the account information using the private key maintained by the browser toolbar; and completing a website form of the web service with a decrypted version of account information.

31. (Previously Presented) The computer readable medium of claim 30, wherein the operations further comprise:

after completing the website form, securely storing the account information at the browser toolbar.

32. (Previously Presented) The computer readable medium of claim 30, wherein the operations further comprise:

removing the account information from the browser toolbar after completing the website form.

33. (Previously Presented) The computer readable medium of claim 30, wherein the operations further comprise:

prior to receiving the encrypted version of the account information, requesting, from a user, access credentials for one or more financial instruments associated with the account holder.

34. (Previously Presented) The computer readable medium of claim 30, wherein the operations further comprise:

based on scheduled intervals, requesting updated account information from the remote database; and

in response to receiving updated account information from the remote database, replacing the account information with the updated account information.

35. (Previously Presented) The computer readable medium of claim 34, wherein requesting the updated account information further comprises:

generating an additional public key pair to encrypt and decrypt the updated account information.

36. (Previously Presented) The computer readable medium of claim 30, wherein the operations further comprise:

loading the decrypted version of account information into an e-wallet usable to provide access to the account information.

37. (Previously Presented) A non-transitory computer readable medium having instructions stored thereon that are executable by a computer system to cause the computer system to perform operations comprising:

determining, at a browser toolbar, that a request for account information has been received from a web service, wherein the account information is usable to conduct a transaction with an account holder;

requesting, by the browser toolbar, the account information from a secure remote database;

performing, by the browser toolbar, decryption on encrypted data received from the remote database to obtain the account information, wherein the decryption uses a cryptographic key generated by the browser toolbar; and

providing, by the browser toolbar, the account information to the web service to facilitate the transaction.

38. (Previously Presented) The computer readable medium of claim 37, wherein the operations further comprise:

generating, by the browser toolbar, a public key pair having a public key and a private key, wherein the cryptographic key is the private key; and

transmitting, by the browser toolbar, the public key to the secure remote database for encrypting the account information.

39. (Previously Presented) The computer readable medium of claim 37, wherein the operations further comprise:

receiving, by the browser toolbar, an additional request from a user to update account information stored by the browser toolbar; and

in response to the additional request:

retrieving, by the browser toolbar, updated account information from the remote database; and

updating, by the browser toolbar, the stored account information with the updated account information.

40. (Previously Presented) The computer readable medium of claim 37, wherein the operations further comprise:

prompting, by the browser toolbar, a user for a security code printed on a transaction instrument associated with the account information, wherein the requesting includes providing the security code the secure remote database.

41. (Previously Presented) The computer readable medium of claim 37, wherein the providing includes populating one or more fields in a web page associated with the web service.

42. (Previously Presented) The computer readable medium of claim 37, wherein the operations further comprise:

after providing the account information to the web service, removing the account information from the browser toolbar.

REMARKS:

Claims 23-42 remain pending in this application.

Section 101 Rejections

All claims are rejected under 35 U.S.C. § 101 as being directed to a judicial exception without reciting significantly more. In particular, the Examiner alleges that the claims are directed to "the concept of secure Internet transactions" and do not recite significantly more than the idea because "[a]ll of [the claimed] computer functions are well-understood, routine, conventional activities previously known to the industry." Office Action 6-8. Applicant respectfully submits that this rejection is improper as set forth below.

First, the alleged abstract idea over generalizes the claimed subject matter. As noted above, the Examiner asserts the claims are directed to "the concept of secure Internet transactions." This attempt to heavily generalize the claimed subject matter is improper as it does not adequately consider the claimed subject matter. In assessing whether the claims are drawn to an abstract idea, the Federal Circuit has "previously cautioned that courts 'must be careful to avoid oversimplifying the claims' by looking at them generally and failing to account for the specific requirements of the claims." *McRo, INC. v. Bandai Namco Games America,* slip op. at 21 (Fed. Cir. September 13, 2016) (citing to *TLI Commc'ns*, 823 F.3d 607, 611 (Fed. Cir. 2016) and *Diehr*, 450 U.S. at 175, 189 n.12 (1981)). As the Federal Circuit explained, "[w]hether at step one or step two of the Alice test, in determining the patentability of a method, a court must look to the claims as an ordered combination, without ignoring the requirements of the individual steps." *Id.* at 21 and 22.

Second, claim 23 recites non-generic computer components performing non-generic computer functions. As discussed below with respect to the § 103 rejections, claim 23 recites "generating, at a browser toolbar, a cryptographic key" and "using, by the browser toolbar, the cryptographic key to decrypt encrypted data [including account information] received from the secure database" "providing, by the browser toolbar, the account information to a web service in response to a request." This specialized "browser toolbar" is new and not taught or suggested by the cited references.

Third, the claimed subject matter is directed to improving the technical field of transaction security. Again, claim 23, for example, recites a specialized "browser toolbar" used in "generating a cryptographic key," "sending ... a request for the account information to a secure database that stores the account information," "using ... the cryptographic key to decrypt encrypted data received from the secure database, wherein the encrypted data includes the account information," "securely storing ... the account information at the browser toolbar," and "providing ... the account information to a web service in response to a request." Relying a specialized browser toolbar to manage account information in this manner potentially reduces the likelihood that the account information becomes compromised. As this is an improvement to the technical field of transaction security, the claims are either not directed to an abstract idea (*see Enfish, LLC v. Microsoft Corp.*, __ F.3d __, slip op. at 10-11 (Fed. Cir. May 12, 2016))[1] or constitute "significantly more" than an abstract idea (*see Bascom Global Internet v. AT&T Mobility LLC*, slip op. at 14 (Fed. Cir. Jun. 27, 2016).

***

Appellant therefore respectfully requests withdrawal of the § 101 rejections of all claims.

Section 103 Rejections

All independent claims are rejected under 35 U.S.C. 103(a) as being unpatentable over Reno, et al. (U.S. Pub. No. 2005/0172229) in view of Weber (U.S. Pub. No. 2004/0061720). Applicant respectfully traverses as set forth below.

Claim 23 recites "generating, at a browser toolbar, a cryptographic key usable to decrypt encrypted account information of an account holder." Claim 23 further recites "using, by the browser toolbar, the cryptographic key to decrypt encrypted data received from the secure database." Reno is alleged to teach these features of claim 23. Office Action at 15 and 16.[2] Applicant respectfully disagrees.

Reno is concerned with preventing "the practice by nefarious parties of fooling a web user into providing sensitive information" through a spoofing website. *See* Reno at ¶ [0003]. As Reno explains, "these fraudulent activities are successful because users are trained to enter

[1] "The Supreme Court has suggested that claims 'purport[ing] to improve the functioning of the computer itself,' or 'improv[ing] an existing technological process' might not succumb to the abstract idea exception. *See Alice*, 134 S. Ct. at 2358–59. While it is true that the Court discussed improvements to computer-related technology in the second step of its analysis in Alice, *see id.* at 2355–60, that was because the Court did not need to discuss the first step of its analysis at any considerable length, *see id.* at 2356 (Petitioner acknowledges that its claims describe intermediate settlement . . . ."), *id.* at 2357."

[2] Weber is not cited for these features and does not appear to include any reference to a cryptographic key.

sensitive information directly into web forms and popup windows. The content and appearance of these windows are easy to spoof since they are based on ordinary HTML." *Id.* Reno thus proposes "a security application that includes at least one data field for receiving input from the user to be sent to a specific resource source" and indicates that "[t]he security application may be a tool bar." *See id.* at ¶¶ [0004] and [0005]. Reno's Fig. 3A, for example, depicts a toolbar for receiving a user's "Online ID" and "Passcode" to access Bank of America's website.

1. *Reno does not teach or suggest "generating, at a browser toolbar, a cryptographic key," as recited in claim 23*

Reno does not appear to include much discussion about using cryptographic keys. In giving examples of sensitive information, Reno indicate that "a user could enter a static or dynamic password to access a local credential (e.g. cryptographic key store, biometric), remote credential (e.g. cryptographic key roaming server) ... ." *Id.* at ¶ [0013]. Reno also discloses that "the security application uses an organization's public key that must be signed and chained to a trusted CA to encrypt the user's sensitive information." *Id.* at ¶ [0035]. Notably, to the extent keys are discussed, however, Reno does not include any discussion about the origin of these keys. Accordingly, Reno does not teach or suggest "<u>generating, at a browser toolbar,</u> a cryptographic key," as recited in claim 23.

2. *Reno does not teach or suggest "decrypt[ing] encrypted data received from the secure database," as recited in claim 23*

Paragraph [0036] is cited for the above-noted feature of claim 23. Office Action at 15. In earlier paragraph [0035], Reno discloses how "the security application uses an organization's public key that must be signed and chained to a trusted CA to encrypt the user's sensitive information." Paragraph [0036] then explains that "<u>the trusted source receives</u> the transmission from the user" and, "[i]f necessary, the source uses its private key to decrypt the transmission" (emphasis). It is important to understand that paragraph [0036] is describing the "trusted source" as being the one receiving information from the "security application," not the security application (corresponding to the alleged "browser toolbar") receiving information from the trusted source. This portion of Reno therefore cannot be said to teach or suggest "using, <u>by the</u>

browser toolbar, the cryptographic key to decrypt encrypted data received from the secure database."

***

Applicant therefore submits that the combination of references does not teach or suggest each and every feature of claim 23. Claim 23 and its dependent claims are therefore patentably distinct over the cited references. Independent claims 30 and 37 (and their respective dependent claims) are believed to also distinguish over the cited references for at least reasons similar to those provided for claim 23.

CONCLUSION:

Applicant respectfully submits the application is in condition for allowance, and an early notice to that effect is requested.

It should also be noted that although arguments have been presented with respect to certain claims herein, the recited subject matter as well as various other subject matter and/or combinations of subject matter may be patentable for other reasons. Further, the failure to address any statement by the Examiner herein should not be interpreted as acquiescence or agreement with such statement. Applicant expressly reserves the right to set forth additional and/or alternative reasons for patentability and/or allowance with the present Application or in any other future proceeding, and to rebut any statement presented by the Examiner in this or other papers during prosecution of the present Application.

If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above-referenced application from becoming abandoned, Applicant hereby petitions for such extension.

The Commissioner is authorized to charge any fees that may be required, or credit any overpayment, to Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C. Deposit Account No. 501505/6857-23203/PTS.

Respectfully submitted,

Date: July 26, 2017

By: /Paul T. Seegers/
Paul T. Seegers
Reg. No. 66,621

Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P. O. Box 398
Austin, Texas 78767
(512) 853-8878